УДК 341.4

О. И. Левшук
доцент кафедры административной деятельности ОВД факультета милиции Академии МВД Республики Беларусь,
кандидат юридических наук, доцент

КИБЕРАТАКИ И МЕЖДУНАРОДНЫЙ ОПЫТ БОРЬБЫ С НИМИ

Обеспечение защиты киберпространства от кибератак со стороны государственных структур, негосударственных субъектов, экстремистских организаций стало в последние годы стратегической задачей большинства стран, которые хотя бы единожды испытали киберугрозы. Так, группировка MuddyWatter пыталась заразить вредоносной программой компьютерные системы израильских компаний, а именно посредством фишинговой рассылки с использованием зараженных документов в форматах PDF и Excel. Целью таких действий было уничтожение данных и причинение экономического ущерба [1, с. 20].

Самыми уязвимыми объектами кибератак являются здравоохранение и образование, социальная сфера, государственные и военные организации. Анализ киберпреступной деятельности на международном уровне показывает, что давольно часто киберугрозы поступают со стороны России, Китая. В частности, в июне 2017 г. компании Украины, Испании и Великобритании неоднократно подверглись кибератакам, которые осуществлялись посредством вредоносной программы под названием «Петя», блокировавшей компьютерные устройства с целью дальнейшего вымогательства денег за разблокировку компьютерных систем [2, с. 22].

Со стороны Китая осуществлялись кибератаки в отношении США и стран Евросоюза. Так, в 2010 г. кибернападение произошло на Google, что привело к краже интеллектуальной собственности. В 2012 г. BAE Systems стала объектом хакеров, которые похитили данные о штурмовиках F-35. В 2015 г. в ходе кибератаки под названием «компьютерный Перл-Харбор» были похищены терабайты секретных данных у предприятий оборонного комплекса США и взломана база данных управления кадров Правительства США. В 2018 г. у поставщика ВМС США были похищены 614 гигабайт данных. В мае 2019 г. китайские хакеры смогли проникнуть в компьютерную систему Агентства национальной безопасности, что позволило им контролировать определенные процессы [3, с. 24]. В ответ на кибератаки со стороны китайских хакеров США укрепило киберподразделения. С 2018 г. успешно функционирует командное управление Министерства обороны США (USCYBERCOM). Недавно в нем появилось 133 новых подразделения: 13 подразделений государственной защиты (защита от массированных атак), 68 подразделе-

ний киберзащиты (защиты основных систем и сетей Министерства обороны), 27 боевых подразделений (проведение скоординированных атак в киберпространстве в качестве поддержки оперативных планов и операций вооруженных сил), 25 подразделений поддержки (аналитика и планирование). Кроме того, создание передовых компьютерных инструментов и инфраструктуры стало приоритетным направлением киберкомандования США (USCYBERCOM), которое стало реализовываться путем создания компьютерных полигонов с использованием облачных технологий [4, с. 5].

В поле зрения киберпреступников за последние годы попадали такие известные компании, как Marriott, Microsoft, Apple, Adobe. Компании, чья система безопасности подвергалась взлому в последние три года, демонстрировали одномоментное падение стоимости активов (около 7,5 %), и на восстановление требовалось более 40 дней. Одной из причин отсутствия надлежащего уровня защиты компьютерных систем (компьютерной информации) стала безграмотность сотрудников компаний в этой сфере.

Как показывает международный опыт, большинство компаний тратит деньги на технический аспект, забывая про человеческий фактор. Между тем 90 % нарушений защиты данных вызваны именно человеческим фактором. Ни одна программа не предотвратит угрозу, нацеленную воспользоваться человеческими слабостями. Речь идет об обучении компьютерной безопасности самих сотрудников компаний. Например, для компании Sky был создан и внедрен проект виртуальной реальности «Свидание с хакером», который позволил ее сотрудникам не только внимательнее относиться к проблемам компьютерной безопасности, но и осознать методы и технику фишинговой рассылки [5, с. 47].

С нехваткой компьютерных специалистов столкнулись правоохранительные и специальные службы Великобритании. 54 % частных компаний и благотворительных фондов, 18 % государственных организаций не имели специалистов даже с базовыми знаниями в области киберпреступности [3, с. 22]. В связи с этим британское правительство разработало Стратегию обучения специалистов для обеспечения национальной кибербезопасности. Ее целью была разработка специальных образовательных программ и стажировка, которые позволили бы подобрать молодых компьютерных специалистов.

С аналогичной проблемой столкнулись ряд государств, которые стали предпринимать попытки привлечь молодежь в сферу кибербезопасности и разведки. Так, в частности, студентам-выпускникам предлагалась полугодовая стажировка, а Европейское агентство по сетевой и информационной безопасности Евросоюза призвало правительства ЕС оказать финансовую помощь выпускникам докторантуры по проблемам кибербезопасности. Израильское правительство для своего раз-

ведывательно-кибернетического подразделения Unit 8200 осуществляло подбор специалистов в сфере кибербезопасности в рамках программы для юных дарований и хакеров из числа выпускников школ. В США подход по повышению компьютерных навыков выражается в предоставлении президентской премии за обучение в сфере кибербезопасности. В будущем планируется тестировать государственных служащих на наличие компьютерных способностей, что, в свою очередь, позволит пройти переподготовку и получить должность в иной государственной организации.

Иным подходом в обеспечении кибербезопасности отличается Дания, которая акцентировала внимание на развитии сенсорных сетей и создании ситуационного центра. На государственном уровне принято решение о вложении значительного капитала в развитие разведывательной службы (Danish Defence Intelligence Service) [6, с. 23].

Таким образом, сегодня мировое сообщество должно быть бдительным и принимать всевозможные меры по недопущению взлома паролей, хищения либо искажения информации, имеющейся в электронных устройствах, вмешательства в работу различных систем посредством сети Интернет, а также совершения иных противоправных действий.

Список основных источников

1. Атака иранских хакеров на израильские компании / пер. С. Велев // Борьба с преступностью за рубежом (по материалам иностранной печати). — 2020. — № 10. — С. 20. Вернуться к статье

2. Гонка кибервооружений: попытка США и НАТО сократить отставание / пер. С. Велев // Борьба с преступностью за рубежом (по материалам иностранной печати). — 2020. — № 4. — С. 20–23. Вернуться к статье

3. Решение проблемы нехватки компьютерных специалистов в правоохранительных органах Великобритании / пер. С. Велев // Борьба с преступностью за рубежом (по материалам иностранной печати). — 2020. — № 1. — С. 21–27. Вернуться к статье

4. Гонка кибервооружений в 2019 году / пер. С. Велев // Борьба с преступностью за рубежом (по материалам иностранной печати). — 2020. — № 1. — С. 3–6. Вернуться к статье

5. Виртуальная реальность и укрепление кибербезопасности в 2020 году / пер. С. Велев // Борьба с преступностью за рубежом (по материалам иностранной печати). — 2020. — № 3. — С. 45–47. Вернуться к статье

6. Обзор киберсистем: продолжение согласованных усилий по адаптации к новым технологиям / пер. С. Л. Семеновой // Иностранная печать об экономическом, научно-техническом и военном потенциале государств — участников СНГ и технических средствах его выявления. — 2020. — № 1. — С. 21–27. Вернуться к статье